

Облікова картка дисертації

I. Загальні відомості

Державний обліковий номер: 0826U004252

Особливі позначки: відкрита

Дата реєстрації: 03-08-2026

Статус: Наказ про видачу диплома

Реквізити наказу МОН / наказу закладу: №336-с від 25.08.2026



II. Відомості про здобувача

Власне Прізвище Ім'я По-батькові:

1. Короткий Тимофій Костянтинович

2. Tymofii K. Korotkyi

Кваліфікація:

Ідентифікатор ORCID ID: 0009-0009-6709-9504

Вид дисертації: доктор філософії

Аспірантура/Докторантура: так

Шифр наукової спеціальності: 126

Назва наукової спеціальності: Інформаційні системи та технології

Галузь / галузі знань:

Освітньо-наукова програма зі спеціальності: Інформаційні системи та технології

Дата захисту: 13-08-2026

Спеціальність за освітою: Комп'ютерна інженерія

Місце роботи здобувача: Золотоныський профейний ліцей

Код за ЄДРПОУ: 02548759

Місцезнаходження: вул Шевченка, Золотоноша, Золотоніський р-н., 19700, Україна

Форма власності: Комунальна

Сфера управління:

Ідентифікатор ROR:

III. Відомості про організацію, де відбувся захист

Шифр спеціалізованої вченої ради (разової спеціалізованої вченої ради): PhD 15075

Повне найменування юридичної особи: Черкаський державний технологічний університет

Код за ЄДРПОУ: 05390336

Місцезнаходження: бульвар Шевченка, Черкаси, Черкаський р-н., 18006, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

IV. Відомості про підприємство, установу, організацію, в якій було виконано дисертацію

Повне найменування юридичної особи: Черкаський державний технологічний університет

Код за ЄДРПОУ: 05390336

Місцезнаходження: бульвар Шевченка, Черкаси, Черкаський р-н., 18006, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

V. Відомості про дисертацію

Мова дисертації: Українська

Коди тематичних рубрик: 20.54.04

Тема дисертації:

1. Ієрхічна інформаційна система моделювання і дослідження алгоритмів потокового SET-шифрування
2. Hierarchical information system for modeling and research of stream SET encryption algorithms

Реферат/анотація:

1. Короткий Т.К. Ієрархічна інформаційна система моделювання і дослідження алгоритмів потокового SET-шифрування. – Кваліфікаційна наукова праця на правах рукопису. Дисертація на здобуття наукового ступеня доктора філософії за спеціальністю 126 «Інформаційні системи та технології». – Черкаський державний технологічний університет, Черкаси, 2026 Дисертаційна робота присвячена підвищенню продуктивності наукових досліджень SET-операцій при побудові перспективних стійких алгоритмів потокового шифрування на основі розширення можливостей ієрархічної інформаційної системи моделювання і дослідження SET-операцій за рахунок встановлення нових і уточнення існуючих взаємозв'язків між моделями ієрархічних рівнів, які в сукупності забезпечать автоматизований синтез і аналіз симетричних та несиметричних однооперандних і багатооперандних SET-операцій, а також генераторів їх псевдовипадкових послідовностей для потокового SET-шифрування. У першому розділі за результатами проведеного аналізу встановлено, що розбудова малоресурсних систем криптографічного захисту інформації на сьогоднішній день відноситься до найбільш актуальних задач розвитку захищених інформаційних і телекомунікаційних

систем. Проаналізовано основні напрямки розвитку і області застосування малоресурсної криптографії. Проведено детальний аналіз відомих результатів дослідження СЕТ-операцій і алгоритмів СЕТ-шифрування, які відносяться до малоресурсної криптографії. Проаналізовано сучасний стан розвитку автоматизованих інформаційних систем моделювання і дослідження СЕТ-операцій та алгоритмів шифрування. Визначено їх переваги і недоліки. За результатами проведеного аналізу сформульована мета і завдання дисертаційного дослідження. Другий розділ присвячений дослідженню особливостей застосування несиметричних двохоперандних СЕТ-операцій, які допускають перестановку операндів в потокових системах шифрування. Проаналізовано два сценарії потокового шифрування, які базуються на використанні комутативних і не комутативних двохоперандних СЕТ-операцій. Наведено структури систем потокового шифрування на основі реалізації даних сценаріїв. Для забезпечення однозначного сприйняття задач і результатів дослідження наводяться основні поняття і визначення стосовно потокового СЕТ-шифрування, які необхідні для даної дисертаційної роботи. На основі реалізації послідовності дискретних перетворень побудована група моделей некомутативних двохоперандних двохранних СЕТ-операцій подвійного циклу, кожна з яких забезпечує перестановку операндів. В основу побудови даної групи було покладено групу СЕТ-операцій з точністю до перестановки результатів перетворення. Дану групу було отримано на основі повного перебору можливих варіантів розміщення 2Ci-квантових однооперандних СЕТ-операцій в 2Ci-квантовій двохоперандній СЕТ-операції. Отримані результати забезпечили можливість удосконалення технології побудови удосконалених моделей некомутативних двохоперандних СЕТ-операцій. Сутність удосконалено полягає в заміні повторного використання технології для знаходження удосконаленої моделі після перестановки операндів на зміну змінних в удосконаленій моделі СЕТ-операції до перестановки операндів. Це забезпечує прямий перехід від моделі СЕТ-операції до перестановки операндів, до моделі СЕТ-операції після перестановки операндів. В третьому розділі запропоновано послідовність перетворень результатів обчислювального експерименту для побудови удосконалених моделей операцій несиметричного криптографічного кодування і декодування. На прикладі однієї з класифікованих множин операцій криптографічного кодування з точністю до перестановки представлених кортежами однооперандних операцій отримано математичні моделі удосконалених несиметричних двохоперандних двохранних операцій подвійного циклу. Запропоновано використати метод синтезу симетричних двохоперандних двохранних операцій для побудови групи несиметричних двохоперандних двохранних операцій. Удосконалений метод синтезу двохоперандних двохранних операцій криптографічного перетворення забезпечив синтез груп несиметричних операцій подвійного циклу. Коректність реалізації даного методу підтверджена класифікованими результатами обчислювального експерименту та збігом отриманих різними методами синтезу математичних моделей на приведеному прикладі однієї з множин операцій. Результати дослідження можливості синтезу множин несиметричних двохоперандних двохранних операцій потрійного циклу показали обмеженість даного методу побудовою лише груп симетричних операцій та несиметричних операцій подвійного циклу. Четвертий розділ присвячено моделюванню множини несиметричних двохоперандних двохранних операцій подвійного циклу на основі дублювання операцій для різних сценаріїв шифрування. Була встановлена можливість синтезу двохоперандних СЕТ-операцій, які допускають перестановку операндів шляхом поєднання однооперандних операцій. Досліджено можливість синтезу множини симетричних двохранних двохоперандних СЕТ-операцій на шляхом поєднання однооперандних операцій

2. Korotkyi T.K. Hierarchical information system for modeling and research of stream SET encryption algorithms. – Qualification scientific work submitted as a manuscript. Dissertation for the degree of Doctor of Philosophy in specialty 126 "Information Systems and Technologies" – Cherkasy State Technological University, Cherkasy, 2026. The dissertation is devoted to improving the efficiency of research on SET-operations in the development of advanced, resilient stream cipher algorithms. The approach is based on expanding the capabilities of a hierarchical information system for modeling and analyzing SET-operations by establishing new and refining existing interrelations between hierarchical models. Collectively, this ensures automated synthesis and analysis of symmetric and asymmetric single-operand and multi-operand SET-operations, as well as generators of their

pseudorandom sequences for stream CET-encryption. In the first chapter, presents an analytical review establishing that the development of resource-efficient cryptographic systems is one of the most pressing challenges in secure information and telecommunication technologies. The chapter surveys the main trends and application areas of lightweight cryptography, providing a detailed analysis of existing research on CET-operations and CET-encryption algorithms in this domain. The current state of automated information systems for modeling and analyzing CET-operations is examined, highlighting strengths and weaknesses. Based on this analysis, the research objectives and tasks of the dissertation are formulated. The second chapter investigates the application of asymmetric two-operand CET-operations permitting operand permutation in stream encryption systems. Two encryption scenarios based on commutative and non-commutative two-operand CET-operations are analyzed, and system structures for their implementation are presented. To ensure clarity, key concepts and definitions relevant to stream CET-encryption are introduced. A group of models of non-commutative two-operand two-bit double-cycle CET-operations was constructed, each supporting operand permutation. The construction was based on a group of CET-operations defined up to the permutation of transformation results, obtained by exhaustively enumerating all possible placements of 2Ci-quantum single-operand operations within a 2Ci-quantum two-operand operation. These results enabled refinement of the technology for constructing advanced models of non-commutative two-operand CET-operations, allowing a direct transition from an operation model to its permuted form by variable substitution rather than repeated application of the synthesis method. In the third chapter, introduces a sequence of transformations of computational experiment results to construct advanced models of asymmetric encryption and decryption operations. Using an example of a classified set of encryption operations (defined up to operand permutation and represented by tuples of single-operand operations), mathematical models of advanced asymmetric two-operand two-bit double-cycle operations were obtained. A method originally intended for synthesizing symmetric two-operand two-bit operations was adapted to construct groups of asymmetric two-operand two-bit operations. The improved synthesis method produced groups of asymmetric double-cycle operations, with correctness validated through classified experimental results and consistency across different synthesis approaches. Further experiments on synthesizing sets of asymmetric two-operand two-bit triple-cycle operations demonstrated limitations of the method, showing that it can construct only groups of symmetric operations and asymmetric double-cycle operations. The fourth chapter focuses on modeling sets of asymmetric two-operand two-bit double-cycle operations through operation duplication for various encryption scenarios. The study confirmed the feasibility of synthesizing two-operand CET-operations that allow operand permutation by combining single-operand operations. The synthesis of symmetric two-bit two-operand CET-operations through such combinations was also explored. Specific attention was given to direct and inverse two-bit two-operand CET-operations permitting operand permutation, constructed either by combining single-operand operations where the first is symmetric or where it is asymmetric. The research established interrelations and constraints characterizing the synthesis of two-bit two-operand cryptographic transformations permitting operand permutation under different models of first-operand transformation. The fifth chapter presents the construction of a hierarchical information system for modeling and analyzing symmetric and asymmetric CET-operations. The central element of a lightweight stream CET-encryption system is a pseudorandom sequence generator of CET-operations defined up to operand permutation. The study of generators of asymmetric operations with second-operand

Державний реєстраційний номер ДіР:

Пріоритетний напрям розвитку науки і техніки: Інформаційні та комунікаційні технології

Стратегічний пріоритетний напрям інноваційної діяльності: Розвиток сучасних інформаційних, комунікаційних технологій, робототехніки

Підсумки дослідження: Новий напрямок у науці і техніці

Публікації:

- Semenov, S., Rudnytskyi, V., Lada, N., Krivtsun, V., Korotkyi, T., Zazhoma, V., & Wasiuta, O. (2026). Stream Encryption Cryptographic Systems Based on Asymmetric Cet Operations with an Accuracy of Permutation. Applied Sciences, No 16 (10), P.
- Rudnytskyi, V., Semenov, S., Lada, N., Babenko, V., Larin, V., Korotkyi T. (2025) The model for constructing a set of symmetric two-operand set operations that allow perversion of operands by combining oneoperand operations. Innovative technologies and scientific solutions for industries, No 3(33), P. 126 – 136
- Rudnytskyi, V., Lada, N., Herashchenko, M., Korotkyi, T., Stebetska, T. (2024) Modeling relationships in noncommutative two-operand two-bit cet-operations of a double cycle when permuting the operands. Technology audit and production reserves. Scientific journal. Vol. 3 No 2(77), 2024. P. 30 – 35
- Ларін В. В., Гусак М. Ю., Короткий Т. К., Гук О. М., Кащишин О. Л. (2025) Моделювання множин двохоперандних трьохрозрядних операцій криптоперетворення шляхом поєднання однооперандних CET-операцій. Збірник наукових праць Харківського національного університету Повітряних Сил. № 1 (83), 2025. С. 56 – 62
- Рудницький С.В., Ларін В.В., Підласий Д.А., Короткий Т.К. (2024) Синтез двохоперандних двоохрозрядних CET-операцій шляхом поєднання однооперандних двоохрозрядних CET-операцій. Наука і техніка Повітряних Сил України. № 4 (57). С.71-79
- Рудницький, В., Бабенко, В., Рудницький, С., Короткий, Т. (2025) Генерація послідовності несиметричних CET-операцій з точністю до перестановки другого операнда. Інформаційні технології та суспільство. № 1 (16), С. 221 – 226
- Рудницький, В. М., Бабенко, В. Г., Рудницький, С. В., Короткий, Т.К., Ковтюх, В. А. (2025) Особливості груп несиметричних CET-операцій синтезованих з точністю до перестановки першого операнда Вчені записки ТНУ імені В.І. Вернадського. Серія: Технічні науки. Том 36 (75) № 4 2025. С. 265-271
- Rudnytskyi, V., Lada, N., Larin, V., Melnyk, O., Stabetska T., Korotkyi T., Pidlasyi D. (2024) Usage of noncommutative two-operand CET-operations in limited resources stream ciphers. Journal of Xidian University. Vol. 18, Issue 5. May 2024. P. 1105 – 1120
- Rudnytskyi, V., Lada, N., Larin, V., Tkachenko, V., Korotkyi, T., Pidlasyi, D., Tarasenko, D. (2024) Information system for modeling and research of pseudorandom sequences of CET-operations for post quantum stream encryption systems. Journal of Xidian University. Vol. 18, Issue 7. July 2024. P. 1284 – 1298.

Наукова (науково-технічна) продукція: технології

Соціально-економічна спрямованість: підвищення автоматизації виробничих процесів

Охоронні документи на ОПВ:

Впровадження результатів дисертації: Впроваджено

Зв'язок з науковими темами:

VI. Відомості про наукового керівника/керівників (консультанта)

Власне Прізвище Ім'я По-батькові:

1. Рудницький Сергій Володимирович

2. Serhii V. Rudnytskyi

Кваліфікація: К. Т. Н., 21.05.01

Ідентифікатор ORCID ID: 0000-0003-3071-7005

Додаткова інформація:

Повне найменування юридичної особи: Черкаський державний технологічний університет

Код за ЄДРПОУ: 05390336

Місцезнаходження: бульвар Шевченка, Черкаси, Черкаський р-н., 18006, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

Власне Прізвище Ім'я По-батькові:

1. Бабенко Віра Григорівна

2. Vira H. Babenko

Кваліфікація: д. т. н., професор, 05.13.05

Ідентифікатор ORCID ID: 0000-0003-2039-2841

Додаткова інформація: <https://scholar.google.com.ua/citations?user=wsrSYZEAAAAJ&hl=uk>; Scopus Author ID: 57433271700

Повне найменування юридичної особи: Черкаський державний технологічний університет

Код за ЄДРПОУ: 05390336

Місцезнаходження: бульвар Шевченка, Черкаси, Черкаський р-н., 18006, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

VII. Відомості про офіційних опонентів та рецензентів

Офіційні опоненти

Власне Прізвище Ім'я По-батькові:

1. Єременко Володимир Станіславович

2. Volodymyr S. Yeremenko

Кваліфікація: д. т. н., професор, 05.13.05

Ідентифікатор ORCID ID: 0000-0002-4330-7518

Додаткова інформація:

Повне найменування юридичної особи: Національний технічний університет України "Київський політехнічний інститут імені Ігоря Сікорського"

Код за ЄДРПОУ: 02070921

Місцезнаходження: проспект Берестейський, Київ, 03056, Україна

Форма власності:

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR: Не застосовується

Власне Прізвище Ім'я По-батькові:

1. Якименко Ігор Зіновійович

2. Ihor Yakymenko

Кваліфікація: к. т. н., доц., 05.13.21

Ідентифікатор ORCID ID: 0000-0003-2586-6196

Додаткова інформація:

Повне найменування юридичної особи: Західноукраїнський національний університет

Код за ЄДРПОУ: 33680120

Місцезнаходження: вул. Львівська, Тернопіль, Тернопільський р-н., 46009, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

Рецензенти

Власне Прізвище Ім'я По-батькові:

1. Палагін Володимир Васильович

2. Volodymyr V. Palahin

Кваліфікація: д. т. н., професор, 01.05.02

Ідентифікатор ORCID ID: 0000-0003-1903-6022

Додаткова інформація:

Повне найменування юридичної особи: Черкаський державний технологічний університет

Код за ЄДРПОУ: 05390336

Місцезнаходження: бульвар Шевченка, Черкаси, Черкаський р-н., 18006, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

Власне Прізвище Ім'я По-батькові:

1. Розломій Інна Олександрівна

2. Inna O. Rozlomii

Кваліфікація: к. т. н., доц., 05.13.05

Ідентифікатор ORCID ID: 0000-0001-5065-9004

Додаткова інформація:

Повне найменування юридичної особи: Черкаський державний технологічний університет

Код за ЄДРПОУ: 05390336

Місцезнаходження: бульвар Шевченка, Черкаси, Черкаський р-н., 18006, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

VIII. Заключні відомості

**Власне Прізвище Ім'я По-батькові
голови ради**

Прокопенко Тетяна Олександрівна

**Власне Прізвище Ім'я По-батькові
головуючого на засіданні**

Прокопенко Тетяна Олександрівна

**Відповідальний за підготовку
облікових документів**

Здобувач PhD

Реєстратор

Юрченко Тетяна Анатоліївна

**Керівник відділу УкрІНТЕІ, що є
відповідальним за реєстрацію наукової
діяльності**



Юрченко Тетяна Анатоліївна